Allen, Dyer, Doppelt,
Milbrath & Gilchrist, P.A.
------ INTELLECTUAL PROPERTY ATTORNEYS ------

255 South Orange Avenue • Suite 1401 • Orlando, FL 32801
Mail to: P. O. Box 3791 • Orlando, FL 32802-3791
tel: 407-841-2330 • fax: 407-841-2343
jabid@addmg.com



# FACSIMILE COVER SHEET

**TO:** Examiner Carl G. COLIN – United States Patent and Trademark Office - Art Unit - 2136

**CLIENT NAME/NUMBER:** 01AG17653537

**TELEPHONE:** 571-272-3682 **FAX NO:** 571-273-8300

**FROM:** Jack G. Abid **DATE:** September 7, 2007

**NUMBER OF PAGES (INCLUDING COVER SHEET):** 22

**COMMENTS/INSTRUCTIONS:**

Please see attached Appeal Brief and for U.S. Patent Application Serial No. 09/974,705.

RECEIVED
CENTRAL FAX CENTER

SEP 0 7 2007

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**
**BEFORE THE BOARD OF APPEALS**

| | |
|---|---|
| In re Patent Application of: **MACCHETTI ET AL.** | Examiner: **Carl G. COLIN** |
| Serial No. **09/974,705** | Art Unit: **2136** |
| Filing Date: **OCTOBER 10, 2001** | Attorney Docket: **53537** |
| For: **METHOD AND CIRCUIT FOR DATA ENCRYPTION/DECRYPTION** | |

**APPELLANTS' APPEAL BRIEF**

MS Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith is Appellants' Appeal Brief together with the requisite $500 large entity fee for filing a brief. If any additional extension and/or fee is required, authorization is given to charge Deposit Account No. **01-0484**.

*(1) Real Party in Interest*

The real party in interest is ST Microelectronics S.R.L., assignee of the present application as recorded at reel 012528, frame 0641.

*(2) Related Appeals and Interferences*

At present there are no related appeals, judicial proceedings, or interferences.

09/10/2007 SSITHIB1 00000062 09974705
01 FC:1402 500.00 OP

RECEIVED
CENTRAL FAX CENTER
SEP 07 2007

In re Patent Application of
**MACCHETTI ET AL.**
Serial No. **09/974,705**
Filed: **OCTOBER 10, 2001**

/

*(3) Status of the Claims*

Claims 21-25, 27-43, and 48-51 are pending in the present application, all stand rejected and are appealed herein.

*(4) Status of the Amendments*

All amendments have been entered and there are no further pending amendments. A copy of the claims involved in this appeal is attached hereto as Appendix A.

*(5) Summary of the Claimed Subject Matter*

Independent Claim 21 is a method of converting data between an unencrypted format **UD** and an encrypted format **ED**, the data being organized in bit words. The method includes converting the data by at least performing a plurality of transformation rounds comprising applying at least one transformation to a two-dimensional array of rows and columns of bit words defining a state array, exchanging each of the rows with a respective column of the state array to form a transposed state array for at least one of the transformation rounds so that the at least one transformation is applied to the transposed state array, and applying at least one round key to the state array in at least one of the transformation rounds. (Figure 6, reproduced below; Specification: page 4, line 15-page 5, line 17; page 9, line 28-page 10, line 20).

Independent Claim 31 is directed to a device **10** for converting data between an unencrypted format **UD** and an encrypted format **ED**. The device comprises a register **24a-d** for storing the

data in the form of bit words, and a circuit **34a-d, 16a-d, 18, 20a-d, 22a-d** for converting the data. The converting comprises performing a plurality of transformation rounds, with each transformation round comprising applying at least one transformation to a two-dimensional array of rows and columns of bit words defining a state array. The converting further comprises exchanging each of the rows with a respective column of the state array to form a transposed state array for at least one of the transformation rounds so that at least one transformation is applied to the transposed state array, and applying at least one round key to the state array in at least one of the transformation rounds. (Figure 6, reproduced below; Specification: page 4, line 15-page 5, line 17; page 9, line 28-page 10, line 20).

Independent Claim 48 is directed to a method of converting data between an unencrypted format **UD** and an encrypted format **ED**, the data being organized in 8-bit words. The method comprises converting the data by at least performing a plurality of transformation rounds for converting the data comprising applying at least one transformation to a two-dimensional array of rows and columns of 8-bit words defining a state array comprising a 4 x 4 matrix of 8-bit words. The transformation round further comprises exchanging each of the rows with a respective column of the state array to form a transposed state array for at least one of the transformation rounds so that the at least one transformation is applied to the transposed state array, and applying at least one round key to the state array in

In re Patent Application of
**MACCHETTI ET AL.**
Serial No. **09/974,705**
Filed: **OCTOBER 10, 2001**

at least one of the transformation rounds. (Figure 6, reproduced below; Specification: page 4, line 15-page 5, line 17; page 9, line 28-page 10, line 20).

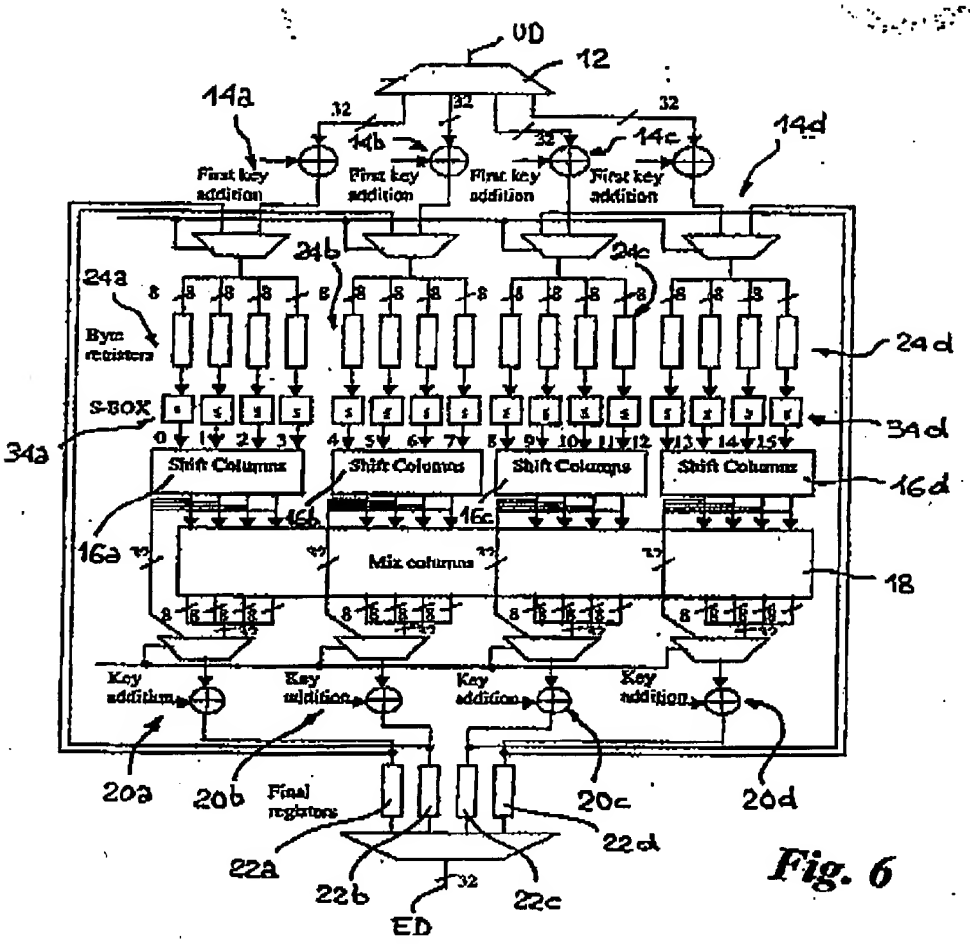


**Figure 6 of the Present Application**

In re Patent Application of
**MACCHETTI ET AL.**
Serial No. **09/974,705**
Filed: **OCTOBER 10, 2001**

*(6) Grounds of Rejection to be Reviewed On Appeal*

The Examiner rejected Claims 21-25, 27-43, and 48-51 under 35 U.S.C. §103(a) over U.S. Patent Publication No. 2001/0024502 to Ohkuma et al. in view of U.S. Patent No. 5,533,127 to Luther.

*(7) Argument*

As will be described in greater detail below, Appellants respectfully submit that the standing rejections of the Examiner are improper and respectfully request that the Board of Patent Appeals and Interferences reverse the Examiner.

The Rejection Over Ohkuma et al. In View of Luther Is Improper

The Examiner rejected independent Claims 21, 31, and 48 over Ohkuma et al. in view of Luther. Ohkuma et al. discloses an apparatus for encrypting blocks of data. (Ohkuma et al.: Paragraphs 10-11). The encryption process occurs in multiple stages. (Paragraph 91-92). Ohkuma et al. also discloses that a matrix may be obtained by substituting rows, substituting columns, and arbitrarily transposing an arbitrary MDS matrix. (Paragraph 268). The Examiner correctly notes that Ohkuma et al. fails to disclose exchanging each of the rows with a respective column of the state array to form a transposed state array, as recited in independent Claims 21, 31, and 48. The Examiner looks to Luther to supply this deficiency.

Luther discloses an encryption system for two-dimensional data. The system of Luther encrypts through multiple

encryption passes performed on binary data. In each pass, the mth row and the nth column of the binary data are encrypted. For each encryption pass, m and n are randomly selected and have a value, which is small relative to the size of the data. (Luther: Col. 1, lines 30-42).

The Examiner contends that steps S211 and S215 of Luther disclose exchanging each of the rows with a respective column of the state array to form a transposed state array, as in the claimed invention. Appellants submit that the Examiner is mischaracterizing Luther. Referencing the code of Luther depicted in Figure 8, reproduced below, and column 5, line 4 through column 6, line 18, in steps S201-202, the random generator is initialized. In step S203, the "StripeHeight" variable is set to a random value between two range values, for example, 1 and 5 (Figure 8).

In re Patent Application of
**MACCHETTI ET AL.**
Serial No. **09/974,705**
Filed: **OCTOBER 10, 2001**

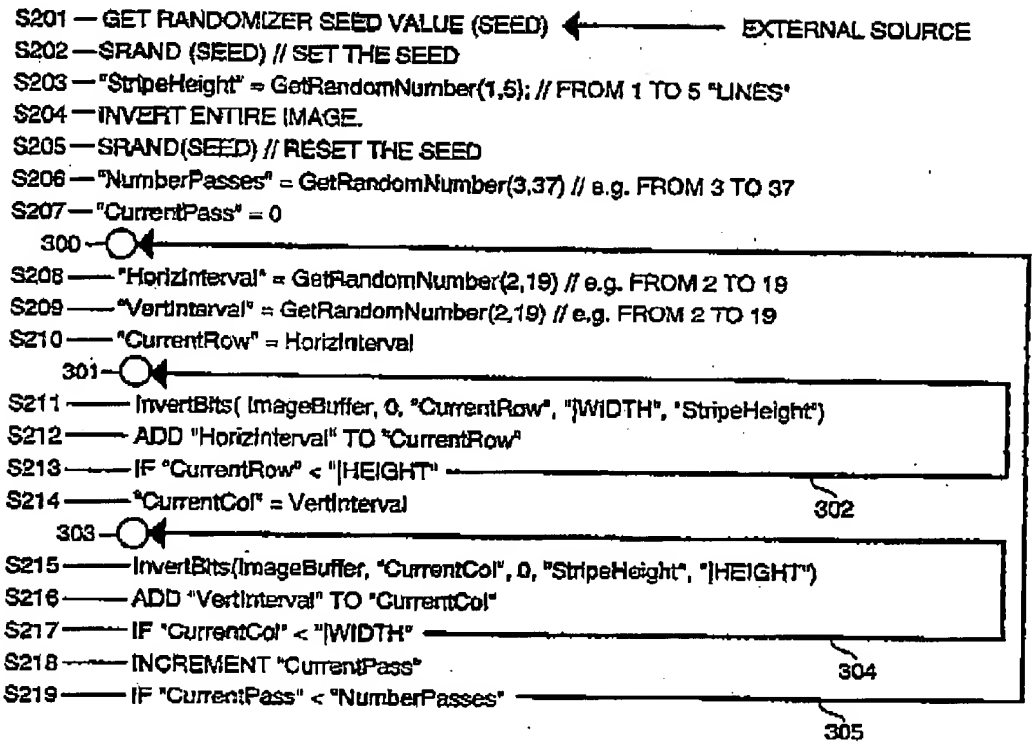


**Figure 8 of Luther**

In step S204, the entire image in the buffer is complemented. The random number generator is reset in step S205. In step S206, the number of encryption passes is randomly set; the "CurrentPass" variable is initialized to zero in step S207. Steps S208 and S209 randomly initialize the "HorizInterval" and "VertInterval" variables, respectively. The "CurrentRow" variable is randomly set in step S210. The invert-bit function (S211) is implemented iteratively.

On the first iteration, the invert-bit function is applied to a 2-dimesnional area of bits defined by the image

width and the randomly set "StripeHeight" variable and located at the first column (0), and a row defined by the "CurrentRow" variable. The "CurrentRow" variable is then incremented by the random "HorizInterval" variable, then if the "CurrentRow" variable is still less than the image height, i.e. not a nonexistent row. The process returns to step S211. In other words, the 2-dimensional area of bits being inverted is moved relatively vertically in the image array by a number of rows equal to the random "HorizInterval" variable. These steps (S211-213) are repeated until the "CurrentRow" variable is greater than or equal to the image height.

In steps S215-217, the invert-bit function is iteratively applied to a 2-dimensional area of bits defined by the image height and the "StripeHeight" variable. The position of application of the invert-bit function moves horizontally across the first row of the array, being iteratively applied to rows. The first column is set in step S214 to the random "VertInterval" variable. The next iteration is applied to a column being incremented by the "VertInterval" variable. This continues on until the "CurrentCol" variable exceeds the image width, i.e. nonexistent column. Thereafter, the "CurrentPass" variable is incremented, and if the appropriate number of passes has not been completed on the image array, the process restarts at step S208.

Appellants note that the invert-bit function does not transpose respective rows and columns, as claimed, but merely complements them. Moreover, for a proper transposition, the

iterations of Luther being applied to the rows first and then columns would have to skip by equivalent intervals. As discussed above, steps S208 and S209 randomly initialize the "HorizInterval" and "VertInterval" variables, respectively. Moreover, Appellants note that Luther does not complement each row/column, but skips a number of rows/columns defined by the random "HorizInterval" and "VertInterval" variables, respectively. Accordingly, the row iterations and column iterations do not match up for a transposition but are instead random.

The Examiner specifically contends that rows 3 and 4 are complemented and columns 4 and 5 are complemented, thereby disclosing the claimed transposition feature. Notwithstanding that complementing does not equal transposing, the Examiner contends that rows 3 and 4 are complemented in Figure 6, and that columns 4 and 5 are complemented in Figure 7. Appellants note that this arrangement of Luther does not disclose the claimed transposition. Rather, the depicted iterations of Luther show complementing of rows 3-4, 6-7, 9-10, 12-13 (Figure 6: StripeHeight = 1, VertInterval =3 [inversion area = image width * (Stripeheight + 1)]) and show complementing of columns 4-5, 8-9, 12-13 (Figure 7: StripeHeight = 1, HorizInterval =4 [inversion area = (Stripeheight + 1)* image height]). This complementing of Luther is derived from the randomly generated "HorizInterval" and "VertInterval" variables.

Therefore, Appellants submit that Luther fails to disclose the claimed feature of exchanging each of the rows with

In re Patent Application of
**MACCHETTI ET AL.**
Serial No. **09/974,705**
Filed: **OCTOBER 10, 2001**

a respective column of the state array to form a transposed state array. Accordingly, it is submitted that independent Claims 21, 31, and 48 are patentable over the prior art. Their respective dependent claims, which recite yet further distinguishing features, are also patentable over the prior art and require no further discussion herein.

In re Patent Application of
**MACCHETTI ET AL.**
Serial No. **09/974,705**
Filed: **OCTOBER 10, 2001**

## CONCLUSIONS

In view of the foregoing arguments, it is submitted that all of the claims are patentable over the prior art. Accordingly, the Board of Patent Appeals and Interferences is respectfully requested to reverse the earlier unfavorable decision by the Examiner.

Respectfully submitted,

JACK G. ABID
Reg. No. 58,237
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
Telephone: 407/841-2330
Fax: 407/841-2343
Attorney for Appellants

In re Patent Application of
**MACCHETTI ET AL.**
Serial No. **09/974,705**
Filed: **OCTOBER 10, 2001**

**CERTIFICATE OF FACSIMILE TRANSMISSION**

I HEREBY CERTIFY that the foregoing correspondence has been forwarded via facsimile number 571-273-8300 to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 this 7 day of September, 2007.

In re Patent Application of
**MACCHETTI ET AL.**
Serial No. **09/974,705**
Filed: **OCTOBER 10, 2001**

## APPENDIX A - CLAIMS ON APPEAL FOR U.S. PATENT APPLICATION SERIAL NO. 09/974,705

21. A method of converting data between an unencrypted format and an encrypted format, the data being organized in bit words, the method comprising:

converting the data by at least performing a plurality of transformation rounds comprising

applying at least one transformation to a two-dimensional array of rows and columns of bit words defining a state array;

exchanging each of the rows with a respective column of the state array to form a transposed state array for at least one of the transformation rounds so that the at least one transformation is applied to the transposed state array; and

applying at least one round key to the state array in at least one of the transformation rounds.

22. A method according to Claim 21 wherein the bit words are 8-bit words.

23. A method according to Claim 21 wherein the state array is a 4 x 4 matrix of bit words.

24. A method according to Claim 21 wherein the plurality of transformation rounds comprises at least 10 transformation rounds.

25. A method according to Claim 21 wherein performing further comprises performing at least one transformation round on a non-transposed state array.

26. (Canceled).

27. A method according to Claim 21 wherein the at least one round key is transposed before being applied to the state array.

28. A method according to Claim 21 further comprising adding code to transpose the at least one round key.

29. A method according to Claim 21 wherein the at least one round key comprises a plurality of round keys, each corresponding to a respective transformation round and being applied according to a round key schedule.

30. A method according to Claim 29 wherein the round key schedule comprises a transposed round key schedule.

31. A device for converting data between an unencrypted format and an encrypted format, the device comprising:

at least one register for storing the data in the form of bit words; and

a circuit for converting the data by at least

performing a plurality of transformation rounds, each transformation round comprising applying at least one transformation to a two-dimensional array of rows and columns of bit words defining a state array,

exchanging each of the rows with a respective column of the state array to form a transposed state array for at least one of the transformation rounds so that at least one transformation is applied to the transposed state array, and

applying at least one round key to the state array in at least one of the transformation rounds.

32. A device according to Claim 31 wherein said at least one register stores bit words as 8-bit words.

33. A device according to Claim 31 wherein said circuit operates on a state array comprising a 4x4 matrix of bit words.

34. A device according to Claim 31 said circuit in performing a plurality of transformation rounds performs at least 10 transformation rounds.

35. A device according to Claim 31 wherein said circuit comprises at least one S-box processing module, said at least one S-box processing module operating on a group of bit words defining a cell of a column of the state array.

36. A device according to Claim 35 wherein the at least one S-box processing module comprises a plurality of S-box modules, each of the plurality of S-box modules operating on a corresponding cell of a column of the state array.

37. A device according to Claim 36 wherein the column of the state array comprises four cells.

38. A device according to Claim 31 wherein the circuit further comprises a plurality of shift column modules, each of said plurality of shift column modules to perform a column shift operation on a column of the state array.

39. A device according to Claim 38 wherein a column shift operation performed by each of said plurality of shift column modules generates shift column data, and wherein said circuit further comprises a single mix column module to perform column mix operations on shift column data.

40. A device according to Claim 31 wherein said circuit is an encoder for converting data from an unencrypted data format to an encrypted data format.

In re Patent Application of
**MACCHETTI ET AL.**
Serial No. **09/974,705**
Filed: **OCTOBER 10, 2001**

41. A device according to Claim 40 wherein said circuit is an embedded system for use in a smart card.

42. A device according to Claim 31 wherein said circuit is a decoder for converting data from an encrypted data format to an unencrypted data format.

43. A device according to Claim 42 wherein said circuit is an embedded system for use in a smart card.

44. (Canceled).

45. (Canceled).

46. (Canceled).

47. (Canceled).

48. A method of converting data between an unencrypted format and an encrypted format, the data being organized in 8-bit words, the method comprising:

converting the data by at least performing a plurality of transformation rounds for converting the data comprising

applying at least one transformation to a two-dimensional array of rows and columns of 8-bit words defining a state array comprising a 4 x 4 matrix of 8-

bit words,

exchanging each of the rows with a respective column of the state array to form a transposed state array for at least one of the transformation rounds so that the at least one transformation is applied to the transposed state array,

applying at least one round key to the state array in at least one of the transformation rounds.

49. A method according to Claim 48 wherein the at least one round key is transposed before being applied to the state array.

50. A method according to Claim 48 further comprising adding code to transpose the at least one round key.

51. A method according to Claim 48 wherein the at least one round key comprises a plurality of round keys, each corresponding to a respective transformation round and being applied according to a round key schedule.

In re Patent Application of
**MACCHETTI ET AL.**
Serial No. **09/974,705**
Filed: **OCTOBER 10, 2001**

## APPENDIX B - EVIDENCE APPENDIX

## PURSUANT TO 37 C.F.R. § 41.37(c)(1)(ix)

None.

In re Patent Application of
**MACCHETTI ET AL.**
Serial No. **09/974,705**
Filed: **OCTOBER 10, 2001**

## APPENDIX C – RELATED PROCEEDINGS APPENDIX PURSUANT TO 37 C.F.R. § 41.37(c)(1)(x)

None.